Journal of Symbolic Computation 35 (2003) 269–279

Journal of Symbolic Computation

www.elsevier.com/locate/jsc

An algorithm to compute the set of characteristics of a system of polynomial equations over the integers

Rosemary Baines, Peter Vámos*

School of Mathematical Sciences, University of Exeter, Laver Building, North Park Road, Exeter EX4 4QE, UK

Received 10 July 2001; accepted 4 October 2002

Abstract

We describe a (finite) algorithm to determine the set of characteristics of a system of polynomial equations with integer coefficients by using the theory of Gröbner bases. This gives us a proof that the set of characteristics must be either finite and not containing zero, or containing zero and co-finite. Another, algebraic, proof of this is given in the appendix. These results carry over to systems of polynomial equations over a principal ideal domain and also yields an algorithm for finding the characteristic set of a matroid.

1. Introduction and background

Given a (finite) system of polynomial equations with integer coefficients, one can decide whether this system is solvable in some field by taking the Gröbner basis of the system over the integers. Our aim in this paper is to show that by using Gröbner bases one can obtain a much richer set of information on the possible fields where this system is solvable, in particular one can determine the possible characteristics of these fields. In matroid theory, the analogous notion of a set of characteristics has been extensively studied and we were led to this problem by trying to find an algorithm to determine the set of characteristics of a matroid. It turns out that the question has a solution in the more general setting of polynomial equations which we will now describe.

All rings in this paper will be commutative. Let $\mathbf{x} = (x_1, x_2, \ldots, x_n)$ be a finite set of indeterminates. We denote the ring of polynomials in n variables over a ring R, $R[x_1, \ldots, x_n]$ by $R[\mathbf{x}]$. Throughout this paper $\mathbb{Z}$ will denote the ring of integers, $\mathbb{Q}$ the field of rational numbers and, for a prime number p, $\mathbb{Z}_p$ will denote the ring of integers

* Corresponding author. Tel.: +44-1392-263-986; fax: +44-1392-263-997.
E-mail addresses: R.A.Baines@ex.ac.uk (R. Baines), P.Vamos@ex.ac.uk (P. Vámos).
URL: http://www.maths.ex.ac.uk/~vamos/.

0014-5793/03/$ - see front matter
doi:10.1016/S0747-7171(02)00134-7

mod p, i.e. the prime field of p elements. Let F denote a system of s polynomial equations in $\mathbb{Z}[\mathbf{x}]$:

$$\begin{aligned} f_1(x_1, \ldots, x_n) &= 0 \\ f_2(x_1, \ldots, x_n) &= 0 \\ &\vdots \\ f_s(x_1, \ldots, x_n) &= 0. \end{aligned} \tag{F}$$

Then the system F can be interpreted in any given field K by extending the canonical homomorphism $\mathbb{Z} \to K$ to a map $\mathbb{Z}[\mathbf{x}] \to K[\mathbf{x}]$ in the natural way. In particular, we may view F as a subset of $\mathbb{Q}[\mathbf{x}]$ via the inclusion map or we may 'reduce F mod p'. When it will be necessary to emphasize the ambient ring in which F is being viewed we will use suffixes, so $F_{\mathbb{Q}}$ and F_p will signify that our system is a subset of the polynomial rings of $\mathbb{Q}[\mathbf{x}]$ and $\mathbb{Z}_p[\mathbf{x}]$ respectively. We will also use the words 'equations' and 'polynomials' interchangeably when referring to the system of equations F or the polynomials $f_1, \ldots, f_s$ respectively.

We wish to find the answers to the questions: 'for what fields K is F solvable when viewed as a system in $K[\mathbf{x}]$ in this way?', and in particular, 'can we determine algorithmically what the primes p are such that there is a field K of characteristic p with F solvable over K?'. These questions lead naturally to the notion of the set of characteristics of the system F which we now make more precise.

Definition. Let $\mathcal{P}_0 = \mathcal{P} \cup \{0\}$, where $\mathcal{P}$ is the set of all primes. Then the set of characteristics of F is defined as

$$\chi(F) = \{p \in \mathcal{P}_0 : F \text{ is solvable in some field of characteristic } p\}.$$

We chose this designation to avoid confusion, in preference to the more natural 'characteristic set', because the latter is already a well-established notion in the theory of Gröbner bases.

To illustrate this notion, consider the system of equations

$$15x - 1 = 0, \qquad 6 = 0.$$

Then $6 = 0$ so $\chi(F) \subseteq \{2, 3\}$ but if K has characteristic 3 then $15x - 1 = 0$ reduces to $-1 = 0$ i.e. $1 = 0$! So the only possibility is solvability over fields of characteristic 2, (indeed the system is solvable over $\mathbb{Z}_2$ with $x = 1$), so we obtain that $\chi(F) = \{2\}$. Note that for a system F, $\chi(F) \neq \varnothing$ if and only if F is solvable in some field. Our main result is the following:

Theorem 1.1. *There is a (finite) algorithm to compute the set of characteristics of a system of equations. In particular, for a given system $F \subseteq \mathbb{Z}[\mathbf{x}]$ as described above, exactly one of the following holds:*

(a) *if $0 \notin \chi(F)$ then $\chi(F)$ is finite;*
(b) *if $0 \in \chi(F)$ then $\chi(F)$ is co-finite (only a finite number of primes are excluded).*

Moreover, all such (finite and co-finite) subsets of $\mathcal{P}_0$ occur as the set of characteristics of some system of equations.

The algorithm, using Gröbner bases over $\mathbb{Z}$, will be given in Section 3; statements (a) and (b) will then be by-products of this algorithm. However, the last statement of Theorem 1.1 is rather trivial so we will get this out of the way now.

Lemma 1.2. *If $T \subseteq \mathcal{P}_0$ is either of the form $0 \notin T$ and $|T| < \infty$, or of the form $0 \in T$ and $|\mathcal{P}_0 \backslash T| < \infty$, then T is the set of characteristics of some system of equations $F \subseteq \mathbb{Z}[\mathbf{x}]$.*

Proof. If T is a finite set of non-zero primes, say $T = \{p_1, \ldots, p_k\} \subseteq \mathcal{P}$, then the single equation $p_1 \ldots p_k = 0$ obviously has set of characteristics T. If T is co-finite, say $T = \mathcal{P}_0 \backslash \{p_1, \ldots, p_k\}$ and x is an indeterminate, then $(p_1 \ldots p_k)x - 1 = 0$ is an equation whose set of characteristics is T. □

Our motivation has been to compute sets of characteristics of matroids. A matroid (also known as a combinatorial geometry) is a finite structure based on the abstraction of dependence/independence in vector spaces, graphs and other algebraic and combinatorial structures. One of the central problems of matroid theory is to represent (or 'coordinatize') a given matroid as a subset of a vector space over some field with the abstract dependence/independence corresponding to linear dependence/independence of the vectors.

Vámos (1971b) showed that the representation problem is equivalent to the solvability of a certain system of polynomial equations in $\mathbb{Z}[\mathbf{x}]$, his result was then further developed by Fenton (1984). According to this scheme, one assigns to a matroid M a matrix whose entries are indeterminates. From this matrix a system of polynomial equations F in $\mathbb{Z}[x_1, \ldots, x_n]$ is obtained by setting the determinants of square submatrices corresponding to non-basis elements of the matroid equal to zero and inverting the product of the square submatrices corresponding to basis elements. The set of fields that this system F is solvable over is exactly the set of fields over which M is representable. For a matroid M the characteristic set (here called the set of characteristics), $\chi(M)$, was defined by Ingleton (1971) and Vámos (1971a) as the set of $p \in \mathcal{P}_0$ for which M is representable over a field of characteristic p. So $\chi(M) = \chi(F)$ for the system F arising from the matroid. The fact that $\chi(M)$ satisfies statement (b) in Theorem 1.1 was shown by Rado (1957) and statement (a) for matroids was proved by Vámos (1971a). Unlike the equation case, the analogue of Lemma 1.2 for matroids is definitely non-trivial and was established by Kahn (1982). For more information about matroids and their representation problem, the reader is referred to Oxley (1992) or Welsh (1976).

From now on we assume that our polynomial equations are arbitrary. The algorithm given in Fig. 1 in Section 3 gives a constructive proof of our main Theorem 1.1, an alternative algebraic proof, applicable in a more general setting, is given in Appendix B. It should be noted that both our main Theorem 1.1 and the algorithm referred to in Theorem 3.5 (and given in detail in Fig. 1 in Section 3) remain valid when $\mathbb{Z}$ is replaced by an arbitrary principal ideal domain (PID). We decided to present the results over $\mathbb{Z}$ rather than a PID mainly because systems arising from matroids, our intended area of application, are integer polynomials, and there is also a hoped for gain in the simplicity of presentation. However, interested readers should have no difficulty adopting the results in this paper to a general PID. Of course the algorithm can only be implemented in those PIDs where Gröbner bases can be effectively computed.

2. Gröbner bases over $\mathbb{Z}$

In order to compute the set of characteristics we will need to know what constants, if any, lie in the ideal of $\mathbb{Z}[\mathbf{x}]$ generated by the polynomials in the system F. The obvious way to do this is to compute a Gröbner basis of this ideal, denoted by $\langle F\rangle$, which will give us a standard form of generating set. Here, and in the rest of this paper we will write $\langle S\rangle$ for the ideal generated by the set S in a ring.

There is much literature on the theory of Gröbner bases over a field and some sources now treat Gröbner bases over more general rings. Since more care needs to be taken when treating Gröbner bases over $\mathbb{Z}$ than over a field, and there is variation in the notation used, we define our notation below and review the main results needed. We will essentially follow Chapter 4 of the book by Adams and Loustaunau (1994) where they treat Gröbner bases for general rings. For all unexplained terms and notions the reader is referred to this text.

Throughout this section we assume that $A = \mathbb{Z}[\mathbf{x}] = \mathbb{Z}[x_1, \ldots, x_n]$. A *monomial* in the variables x_i is an expression of the form $x_1^{\alpha_1} x_2^{\alpha_2} \ldots x_n^{\alpha_n}$ where $\alpha_1, \ldots, \alpha_n \in \mathbb{N}$, and we will write this in the abbreviated form: $\mathbf{x}^{\boldsymbol{\alpha}}$, where $\boldsymbol{\alpha} = (\alpha_1, \ldots, \alpha_n) \in \mathbb{N}^n$. Gröbner bases depend on a total ordering of the monomials which extend the natural divisibility order, such an ordering will be implicitly assumed throughout and will only be specified in the computational examples in Appendix A. We use the word *term* for a monomial multiplied by a non-zero constant, $a\mathbf{x}^{\boldsymbol{\alpha}}$, $0 \neq a \in \mathbb{Z}$. For a polynomial $f \in \mathbb{Z}[\mathbf{x}]$ we refer to the *lead monomial* (lm) and *lead term* (lt) respectively for the largest monomial (term) with non-zero coefficient with respect to the monomial order occurring in f, and denote by lc the lead coefficient.

A polynomial, $f \in A$ may be reduced by a set of non-zero polynomials $F \subseteq A$. We denote a one step reduction by $f \xrightarrow{F} h$, reduction in more than one step by $f \overset{F}{\rightsquigarrow} h$ and when we wish to show that h cannot be further reduced modulo F then we will denote this by $f \overset{F}{\rightsquigarrow}_+ h$.

Our main use of Gröbner bases will be the fact that they allow us to compute the constants in an ideal of A. More precisely, if G is a Gröbner basis for an ideal $I \subseteq A$ then $I \cap \mathbb{Z} = \langle G \cap \mathbb{Z}\rangle$. Note that this fact does not depend on the particular monomial order chosen. It is easy to see that if G is a Gröbner basis in A whose constant polynomials are $c_1, \ldots, c_k \in \mathbb{Z}$, then the set $(G \backslash \{c_1, \ldots, c_k\}) \cup \gcd(c_1, \ldots, c_k)$ is also a Gröbner basis for the same ideal with just one constant term. So we may assume that if a Gröbner basis contains any constants then it contains just one positive constant. Indeed, this constant will be unique, irrespective of the term order chosen and whatever the Gröbner basis found, in view of the comment above, since it is the (unique non-negative) generator of the ideal $I \cap \mathbb{Z}$. In the rest of this paper we will tacitly assume that our Gröbner bases will always have this property.

The computational test for a set of polynomials to be a Gröbner basis over a field involves forming, for a pair of polynomials, Buchberger's S-polynomial. The more general definition applicable in $\mathbb{Z}[\mathbf{x}]$ is given below.

Definition. Consider two non-zero polynomials $f_1, f_2 \in \mathbb{Z}[\mathbf{x}]$. Let the leading terms be $\mathrm{lt}\, f_i = c_i \mathbf{x}_i^{\boldsymbol{\alpha}}$ where $c_i \in \mathbb{Z}$ and $\mathbf{x}_i^{\boldsymbol{\alpha}}$ is the leading monomial of f_i, $i = 1, 2$. Let

$c = \operatorname{lc m}(c_1, c_2)$ and $\mathbf{x}^{\boldsymbol{\alpha}} = \operatorname{lc m}(\mathbf{x}_1^{\boldsymbol{\alpha}}, \mathbf{x}_2^{\boldsymbol{\alpha}})$ so that $\operatorname{lc m}(\operatorname{lt} f_1, \operatorname{lt} f_2) = c\,\mathbf{x}^{\boldsymbol{\alpha}}$. Then we define the *S-polynomial* of f_1 and f_2 to be

$$S(f_1, f_2) = \frac{c}{c_1}\frac{\mathbf{x}^{\boldsymbol{\alpha}}}{\mathbf{x}_1^{\boldsymbol{\alpha}}} f_1 - \frac{c}{c_2}\frac{\mathbf{x}^{\boldsymbol{\alpha}}}{\mathbf{x}_2^{\boldsymbol{\alpha}}} f_2.$$

We note that the key role of S-polynomials in the test for Gröbner bases is still valid in this context.

Theorem 2.1 (Buchberger's Theorem). *Let $G = \{g_1, \ldots, g_s\}$ be a set of non-zero polynomials in $A = \mathbb{Z}[\mathbf{x}]$. Then G is a Gröbner basis if and only if for every $i \neq j \in \{1, \ldots, s\}$, $S(g_i, g_j) \overset{G}{\rightsquigarrow}_+ 0$.*

Proof. See Proposition 4.5.3 and Algorithm 4.5.1 in Adams and Loustaunau (1994). □

3. The algorithm

Let $F \subseteq \mathbb{Z}[\mathbf{x}]$ be a system of polynomials as described in Section 1 and let the ideal they generate be $I = \langle F \rangle$. Recall that for any field K, we may interpret F as lying over K via the canonical map $\mathbb{Z}[\mathbf{x}] \to \mathbb{Z}[\mathbf{x}] \otimes_{\mathbb{Z}} K \backsimeq K[\mathbf{x}]$ which sends $1 \mapsto 1_K$. We denote by F_K the system of equations, F, when viewed over the polynomial ring $K[\mathbf{x}]$ and let I_K be the image of I under this map (the ideal generated by F_K in $K[\mathbf{x}]$).

Recall that Hilbert's Nullstellensatz tells us that F_K is solvable over some extension of K if and only if $1 \notin I_K$. Since K is a field, for all non-zero constants $k \in K$, if $k \in I_K$ then $1 \in I_K$. Further, $1 \in I$ will mean that $1 \in I_K$ for all fields K whence $\chi(F) = \varnothing$. We note this in the following lemma.

Lemma 3.1. *If F is a system of polynomials in $\mathbb{Z}[\mathbf{x}]$ whose Gröbner basis contains the constant polynomial 1 then $\chi(F) = \varnothing$.*

There are now two other possibilities to examine: either I contains no constant terms, or I contains non-zero constants, none of which are 1.

Definition. Let $k \in \mathbb{Z}$, $k > 1$, then we define the *primes of k* to be the set $\operatorname{pri} k = \{p \in \mathcal{P} : p \mid k\}$.

Lemma 3.2. *If F is a system of polynomials in $\mathbb{Z}[\mathbf{x}]$ such that a Gröbner basis G for $\langle F \rangle$ contains the unique constant $k > 1$ then $\chi(F) = \operatorname{pri} k$.*

Proof. It is obvious that $\chi(F) \subseteq \operatorname{pri} k$. Let $p \in \operatorname{pri} k$, with $pp' = k$. Let F_p denote the system of polynomials F, interpreted over $\mathbb{Z}_p$. Then we see that $p \notin \chi(F)$ if and only if $1 \in \langle F_p \rangle$, i.e. there is an $f \in \mathbb{Z}[\mathbf{x}]$ such that $pf - 1 \in I$. Then $p' = kf - p'(pf - 1) \in \langle G \rangle \cap \mathbb{Z}$ so $k \mid p'$ which is a contradiction. Hence $p \in \chi(F)$, and $\chi(F) = \operatorname{pri} k$ as required. □

It now remains to consider the case when G contains no constant terms, i.e. when $\deg g > 0$ for all $g \in G$. In this case, since G is still a Gröbner basis when considered in $\mathbb{Q}[\mathbf{x}]$, we know that $1 \notin I_{\mathbb{Q}}$ and hence $0 \in \chi(F)$.

Let $p \in \mathcal{P}$, then we note that, interpreting I as an ideal in $\mathbb{Z}_p[\mathbf{x}]$ is equivalent to adding the equation $p = 0$ to our equations i.e. adding the polynomial p to the generators of I. We ask: when will the set $G \cup \{p\}$ still be a Gröbner basis? If $G \cup \{p\}$ is a Gröbner basis then clearly $p \in \chi(F)$. Recall that G_p denotes the image of G mod p, i.e. the set of all polynomials in G reduced mod p. Note that the question whether the image of a Gröbner basis remains a Gröbner basis or not under the passage of a ring homomorphism i.e. under an 'extension of scalars' is considered in Bayer et al. (1993). The simple case needed here is set out in the following lemma.

Lemma 3.3. *If $p \nmid \operatorname{lc} g$ for all $g \in G$, then $G \cup \{p\}$ is still a Gröbner basis in $\mathbb{Z}[\mathbf{x}]$ (equivalently, G_p is a Gröbner basis in $\mathbb{Z}_p[\mathbf{x}]$).*

Proof. From Buchberger's theorem (Theorem 2.1), we know that $G \cup \{p\}$ is a Gröbner basis if and only if all the S-polynomials of pairs in this set reduce to zero. We observe that for any pair $g_i, g_j \in G$, $S(g_i, g_j) \overset{G}{\rightsquigarrow}_+ 0$ implies that $S(g_i, g_j) \overset{G\cup\{p\}}{\rightsquigarrow}_+ 0$, so it only remains to test that for all $g \in G, S(g, p) \overset{G\cup\{p\}}{\rightsquigarrow}_+ 0$. This follows since for all $g \in G, S(g, p) = pg - p \operatorname{lt} g = p(g - \operatorname{lt} g) \overset{p}{\to} 0$. □

We have now shown that in the case when $G \cap \mathbb{Z} = \varnothing$, we must have $0 \in \chi(F)$ and there are at most a finite number of primes excluded from $\chi(F)$. Hence the set of characteristics is co-finite in this case and we can specify it in terms of the primes that are excluded. We call these the 'bad primes' of F and denote them by $\eta(F)$, so in this case $\chi(F) = \mathcal{P}_0 \backslash \eta(F)$. We also know from Lemma 3.3 above that $\eta(F) \subseteq \{p \in \mathcal{P} : p \mid \operatorname{lc} g_i \text{ for some } 1 \leq i \leq s\}$ and naively we may test each of these cases separately by recomputing the Gröbner basis of G_p over the field $\mathbb{Z}_p$ for each bad prime p. In fact, the following lemma gives us a method for determining $\eta(F)$ in just one more step.

Lemma 3.4. *Let $F \subseteq \mathbb{Z}[\mathbf{x}]$ be such that a Gröbner basis $G = \{g_1, \ldots, g_s\}$ for F has $\deg g_i > 0, 1 \leq i \leq s$, (i.e. $G \cap \mathbb{Z} = \varnothing$). Set $\gamma = \operatorname{lc} \operatorname{m}(\operatorname{lc} g_1, \ldots, \operatorname{lc} g_s)$. Then, regarding γ as a constant polynomial, any Gröbner basis G' of the set $G \cup \{\gamma\}$ must have a constant polynomial (recall that this is unique and positive by our convention). Setting $k' = G' \cap \mathbb{Z}$, $\eta(F) = \operatorname{pri} \gamma \backslash \operatorname{pri} k'$ follows.*

Proof. As we have already noted, it follows from Lemma 3.3 and by the construction of γ, that $\eta(F) \subseteq \operatorname{pri} \gamma$.

Regard γ as a constant polynomial and let G' be a Gröbner basis for the set $G \cup \{\gamma\}$. Set $I' = \langle G' \rangle \subseteq \mathbb{Z}[\mathbf{x}]$. Then, since $\gamma \in I'$, G' must contain at least one non-zero constant term and, as before, we can insist that there is only one constant term which is positive. Obviously this constant term, which we denote by k' must divide γ.

Now it is clear that $I' \supseteq I$ and $\chi(G') \subseteq \chi(G) = \chi(F)$. Also, $\chi(G') = \operatorname{pri} k'$ by Lemma 3.2. Therefore $\operatorname{pri} k' \subseteq \chi(G)$.

Hence we have shown that $\eta(F) \subseteq \text{pri}\ \gamma \backslash \text{pri}\ k'$ and it remains to show that all the primes which 'disappear' on computing G' are in fact bad. Consider such a disappearing prime $p \in \mathcal{P}$ with $p \mid \gamma$ but $p \nmid k'$. Then, regarding p as a constant polynomial, look at the set $G \cup \{p\}$. Now any Gröbner basis G^* of $G \cup \{p\}$ must also have a constant polynomial (since $p \in \langle G^* \rangle$) and the only possibilities for this are 1 and p (the divisors of p). Assume for contradiction that the constant polynomial was p, then by Lemma 3.2 we know that $\chi(G^*) = \{p\}$. Let K be some field where G^* is solvable, then since K has characteristic p, $\gamma = 0$ in K also, so G' must be solvable over K as well and hence $p \in \chi(G') = \text{pri}\ k'$, contradicting the fact that $p \nmid k'$. So $G^* \cap \mathbb{Z} = \{1\}$ and $p \in \eta(F)$ as required. □

We note that when we recompute the Gröbner basis in this case and find that $k' = 1$ then $\text{pri}\ k' = \varnothing$ and hence $\eta(F) = \text{pri}\ \gamma$.

Theorem 3.5. *The algorithm given in Fig. 1 below is a finitely terminating algorithm which exactly determines the set of characteristics of F.*

INPUT: A set of non-zero polynomials $F = \{f_1, \ldots, f_t\} \subseteq \mathbb{Z}[\mathbf{x}]$.
OUTPUT: $\chi(F)$, the set of characteristics of F.
STEP 1: Compute the Gröbner Basis, G, of F over $\mathbb{Z}$.
STEP 2: Compute the intersection $= G \cap \mathbb{Z}$;
either a unique, positive constant k, or empty.
STEP 3:
IF k $= 1$
THEN $\chi(F) = \varnothing$
IF k > 1
THEN $\chi(F) = \text{pri}\ k$
ELSE (when $G \cap \mathbb{Z} = \varnothing$)
Set $\gamma := \text{lcm}\{\ \text{lc}\, g : g \in G\ \}$
Compute the Gröbner Basis, G' of $G \cup \{\gamma\}$ (in $\mathbb{Z}[\mathbf{x}]$)
Find the new constant term, $k' = G' \cap \mathbb{Z}$
THEN $\eta(F) = \text{pri}\ \gamma \setminus \text{pri}\ k'$ and
$\chi(F) = \mathcal{P}_0 \setminus \eta(F) = (\mathcal{P}_0 \setminus \text{pri}\ \gamma) \cup \text{pri}\ k'$.

Fig. 1. Algorithm for computing the set of characteristics.

Proof. This algorithm must terminate, since computing a Gröbner basis (which we do at most twice) uses a finite algorithm. It is also possible to compute the intersection of G with $\mathbb{Z}$ (when eliminating all variables, any order is an elimination order) and we can insist that this intersection must either be empty, or a unique, positive constant by the form of G chosen.

That the output is indeed the set of characteristics of F follows from Lemmas 3.1, 3.2 and 3.4. □

Proof (Theorem 1.1). This now follows from Theorem 3.5. □

Acknowledgements

The research of the first author is supported by a CASE award from EPSRC and GCHQ.

Appendix A. Examples

We have implemented our algorithm on the computer algebra system Macaulay 2 (Grayson and Stillman, 2000). We have used this system because it can handle the computation of Gröbner bases over the integers for sets of homogenous equations. The following examples were computed on Macaulay 2 by introducing an extra homogenizing variable, h, then dehomogenizing after the Gröbner basis has been computed. Throughout, the ordering of the monomials used was DegLex with $x > y > z > w$.

Example 1. $F_1 = \{x^2 + xy, y - 1, x - 3y + 3, y - 9x\} \subseteq \mathbb{Z}[x, y]$ has a Gröbner basis $G_1 = \{1\}$ so $\chi(F_1) = \varnothing$.

Example 2. A Gröbner basis of the set $F_2 = \{xy^4 - 2x^3y + 5, y^3 - 2x^2, x^2y, w^3 + (x - 1)^2x^2y - 22y^4x^4, 2x^4, (x - y)(y^3 - 2x^2) - 14x^4\} \subseteq \mathbb{Z}[x, y, z, w]$ is $G_2 = \{x^2y, y^3 - 2x^2, 2x^4, 5, w^3\}$ with $G_2 \cap \mathbb{Z} = \{5\}$ and so $\chi(F_2) = \text{pri } 5 = \{5\}$.

Example 3. $F_3 = \{4x^2y^2 + 2xy^3 + 3xy, 2x^2 + xy, 2y^2\} \subseteq \mathbb{Z}[x, y]$ has a Gröbner basis $G_3 = \{2x^2 + xy, 2y^2, xy^3, 3xy\}$ so $G_3 \cap \mathbb{Z} = \varnothing$. Then $\text{lc m}(2, 2, 1, 3) = 6$ and the set $G_3 \cup \{6\}$ has Gröbner basis $G_3' = \{6, 2x^2 + xy, 3xy, 2y^2\}$ with $G_3' \cap \mathbb{Z} = \{6\}$. Therefore $\eta(F_3) = \varnothing$ and $\chi(F_3) = \mathcal{P}_0$.

Example 4. $F_4 = \{2wy^3 + 30x + 5, y^3, 6xy^6 + 3yw^2\} \subseteq \mathbb{Z}[x, y, z, w]$ has a Gröbner basis $G_4 = \{y^3, 30x + 5, yw^2\}$ so $G_4 \cap \mathbb{Z} = \varnothing$ and $\gamma = \text{lc m}(1, 30, 1) = 30$. Then $G_4 \cup \{\gamma\}$ has Gröbner basis $\{5, y^3, yw^2\}$ so $\eta(F_4) = \text{pri } 30 \backslash \text{pri } 5 = \{2, 3, 5\} \backslash \{5\} = \{2, 3\}$ and so $\chi(F_4) = \mathcal{P}_0 \backslash \{2, 3\}$ which is co-finite.

It is standard matroid theory that the Fano matroid is representable over a field if and only if the field has characteristic 2 and the non-Fano matroid is representable over a field exactly when it has characteristic other than 2 (see Oxley, 1992, p. 505). In the following two examples, we find a system of equations that is representable exactly when the matroid is using the method discussed in Fenton (1984).

Example 5 (Fano Matroid). The Fano matroid is representable exactly when the following equations in $\mathbb{Z}[x_1, x_2, x_3, w]$ are solvable:

$$\{(x_1x_2 - x_2 + 1)(x_1x_3 - x_1 - x_3)(x_2 + x_3 - 1)x_1^5x_2^5x_3^5w - 1,$$
$$x_1 - 1, x_2 - 1, x_3 - 1, x_1x_2 + x_3\}.$$

A Gröbner basis for this set of polynomials is

$$\{x_1 - 1, x_2 - 1, x_3 - 1, 2, w + 1\}$$

and so we see that the set of characteristics of the Fano matroid is $\{2\}$, as expected.

Example 6 (Non-Fano Matroid). We compare the last example with that of the non-Fano matroid, which give rise to the system of polynomials,

$$\{(x_1x_2 - x_2 + 1)(x_1x_3 - x_1 - x_3)(x_2 + x_3 - 1)(x_1x_2 + x_3)x_1^5x_2^5x_3^5w - 1,\\ x_1 - 1, x_2 - 1, x_3 - 1\}$$

in $\mathbb{Z}[x_1, x_2, x_3, w]$ which has a Gröbner basis

$$\{x_1 - 1, x_2 - 1, x_3 - 1, 2w + 1\}$$

so the non-Fano matroid has a co-finite set of characteristics since $(G \cap \mathbb{Z}) = 0$. Thus $\gamma = \text{lc m}(1, 1, 1, 2) = 2$. When we add 2 to the Gröbner basis and run the Gröbner basis algorithm again we find a Gröbner basis to be just the set

$$\{x_1 - 1, x_2 - 1, x_3 - 1, 2w + 1, 2\}.$$

So our algorithm confirms that the non-Fano matroid indeed has set of characteristics $\mathcal{P}_0\backslash\{2\}$.

Appendix B. Algebraic proofs

Our algorithm gives a constructive proof that the set of characteristics is either finite or co-finite in $\mathcal{P}_0$. We will now show how this result could be deduced from a much more general and deeper theorem of Chevalley in commutative algebra (see Matsumura, 1980, Theorem 6 or Eisenbud, 1995, Corollary 14.7), using the notion of a constructible set of prime ideals of our base ring. Note, however, that the proof is not constructive so not surprisingly, it will not yield an algorithm. Henceforth all rings will be commutative and Noetherian in this section.

For a ring S, we denote the set of prime ideals of S by Spec S (the spectrum of S) and min B will denote the subset of minimal prime ideals of $B \subseteq$ Spec S. Then Spec S is a topological space in the usual Zariski (hull-kernel) topology; the *closed* sets of Spec S are of the form

$$V(I) = \{P \in \text{Spec } S : P \supseteq I\} \qquad \text{where } I \text{ is an ideal of } S.$$

It is clear that $V(I)$ can be identified with Spec R/I. We also note that our $\mathcal{P}_0$ as defined in Section 1 can be identified with Spec $\mathbb{Z}$. A subset $C \subseteq$ Spec S is said to be *constructible* if it is a finite union of sets which are the intersections of a closed and an open subset of Spec S:

$$C = (U_1 \cap F_1) \cup \cdots \cup (U_k \cap F_k), \qquad U_i \text{ open } F_i \text{ closed } 1 \leq i \leq k.$$

Clearly, every open or closed set is constructible, also the constructible subsets of Spec S are closed under finite unions, intersections and taking complements, see Matsumura (1980, Section 6) for the details. Fix a non-trivial ring R and let S be an R-algebra. Then the canonical ring homomorphism

$$f : R \to S \qquad r \mapsto r.1_S \tag{B.1}$$

induces a (continuous) map

$$f^* : \text{Spec } S \to \text{Spec } R \qquad Q \mapsto f^{-1}(Q), \qquad Q \in \text{Spec } S. \tag{B.2}$$

We define the (R-)set of characteristics of S to be

$$\chi_R(S) = f^*(\text{Spec } S) = \{ f^*(Q) : Q \in \text{Spec } S\} \subseteq \text{Spec } R.$$

If $R = \mathbb{Z}$ and F is a set of polynomials in $A = \mathbb{Z}[\mathbf{x}]$ then we recover our original definition of the set of characteristics of F by passing to the factor ring of A by $\langle F\rangle$. In fact, $\chi_{\mathbb{Z}}(A/\langle F\rangle) = \chi(F)$ as defined in Section 1, so our definition is indeed a generalization of our earlier one. In general, $\chi_R(S)$ is neither open nor closed in Spec R. However we have the important result of Chevalley mentioned above:

Theorem B.1. *Let R be a (Noetherian) ring, let S be an affine R-algebra (i.e. a factor of the polynomial ring $R[x_1, \ldots, x_n]$) and let f be the canonical ring homomorphism $f : R \to S$. Then f^* (as given in (B.2)) maps constructible sets of* Spec S *to constructible sets of* Spec R. *In particular, $\chi_R(S)$ is a constructible set in* Spec R.

Proof. See Matsumura (1980, Theorem 6, Section 6.E) or Eisenbud (1995, Corollary 14.7). □

Using the above theorem we can deduce our main result Theorem 1.1, by characterizing the constructible sets of Spec R when d R is a PID as the sets of characteristics as given in Theorem 1.1. We will do this in the slightly more general setting of domains of dimension 1.

Theorem B.2. *Let R be a Noetherian domain of Krull dimension* 1. *Then a subset $C \subseteq$* Spec R *is constructible (in* Spec R*) if and only if it is either finite and does not contain the* 0 *ideal, or co-finite (in* Spec R*) and contains the* 0 *ideal.*

Proof. Let R be a Noetherian domain of Krull dimension 1 and put $\Pi =$ Spec R and let $C \subseteq \Pi$. In this case every non-zero prime of R is maximal and there are only finitely many maximal ideals containing a non-zero ideal. It follows that the closed sets in Π are exactly the finite sets not containing 0 and Π itself, whence the open sets are the co-finite set containing 0 and the empty set $\varnothing$. Hence the finite sets not containing 0 and the co-finite set containing 0 are all constructible. Further, the intersection of a closed and an open set is again of the form of a finite set not containing 0 or a co-finite sets containing 0 and clearly these sets are closed under finite unions. So every constructible set of Π is either a finite set not containing 0 or a co-finite sets containing 0, as claimed. □

Corollary B.3. *Let R be a Noetherian domain of Krull dimension* 1 *(in particular a PID), and let S be an affine R-algebra (i.e. a factor of the polynomial ring $R[x_1, \ldots, x_n]$). Then $\chi_R(S)$ is either finite and does not contain* 0 *or co-finite (in* Spec R*) and contains* 0.

Proof. Combine Theorems B.1 and B.2. □

References

Adams, W.W., Loustaunau, P., 1994. An Introduction to Gröbner Bases, American Mathematical Society, Providence, RI.

Bayer, D., Galligo, A., Stillman, M., 1993. Gröbner bases and extension of scalars. In: Computational Algebraic Geometry and Commutative Algebra (Cortona, 1991), Cambridge University Press, Cambridge, pp. 198–215.

Eisenbud, D., 1995. Commutative Algebra, Springer-Verlag, New York. With a view toward algebraic geometry.

Fenton, N.E., 1984. Matroid representations—an algebraic treatment. Quart. J. Math. Oxford Ser. (2) 35 (139), 263–280.

Grayson, D.R., Stillman, M.E., 2000. Macaulay 2, a software system for research in algebraic geometry. Available from http://www.math.uiuc.edu/Macaulay2.

Ingleton, A.W., 1971. Representation of matroids. In: Combinatorial Mathematics and its Applications (Proc. Conf., Oxford, 1969), Academic Press, London, pp. 149–167.

Kahn, J., 1982. Characteristic sets of matroids. J. London Math. Soc. (2) 26 (2), 207–217.

Matsumura, H., 1980. Commutative Algebra, second ed, Benjamin/Cummings Publishing Co., Inc., Reading, MA.

Oxley, J.G., 1992. Matroid Theory, The Clarendon Press, Oxford University Press, New York.

Rado, R., 1957. Note on independence functions. Proc. London Math. Soc. (3) 7, 300–320.

Vámos, P., 1971a. Linearity of matroids over division rings. In: Möbius Algebras (Proc. Conf., Univ. Waterloo, Waterloo, ON, 1971), University of Waterloo, Waterloo, ON, pp. 170–174. Notes by G. Roulet.

Vámos, P., 1971b. A necessary and sufficient condition for a matroid to be linear. In: Möbius Algebras (Proc. Conf., Univ. Waterloo, Waterloo, ON, 1971), University of Waterloo, Waterloo, ON, pp. 162–169.

Welsh, D.J.A., 1976. Matroid Theory, L.M.S. Monographs, No. 8, Academic Press (Harcourt Brace Jovanovich Publishers), London.